[10191/3602]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

Inventor(s)	:	Jochen WEBER et al.
Serial No.	:	10/801,363
Filed	:	March 15, 2004
For	:	MICROPROCESSOR SYSTEM AND METHOD FOR DETECTING THE EXCHANGE OF MODULES OF THE SYSTEM
Examiner	:	Fatoumata TRAORE
Art Unit	:	2136
Confirmation No.	:	3174

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Date: September 2, 2008

Signature: _____
Jong H. Lee (Reg. No. 36,197)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' APPEAL BRIEF
UNDER 37 C.F.R. § 41.37

S I R :

Applicants filed a Notice of Appeal dated April 7, 2008, appealing from the Final Office Action dated November 7, 2007, in which claims 1-19 of the above-identified application were finally rejected. This Appeal Brief is submitted by Applicants in support of their appeal.

I. REAL PARTY IN INTEREST

The real party in interest in the present appeal is Robert Bosch GmbH of Stuttgart, Germany. Robert Bosch GmbH is the assignee of the entire right, title, and interest in the present application.

II. RELATED APPEALS AND INTERFERENCES

No appeal or interference which will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the pending appeal is known to exist to the undersigned attorney or is believed by the undersigned attorney to be known to exist to Applicants.

III. STATUS OF CLAIMS

Claims 1-19 are currently pending in the present application and claims 1-19 are being appealed. Among the claims being appealed, claims 1 and 10 are independent; claims 2-9 ultimately depend on claim 1; and claims 11-19 ultimately depend on claim 10.

IV. STATUS OF AMENDMENTS

No amendment has been made subsequent to the final Office Action mailed on November 7, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

With respect to independent claim 1, the present invention provides a microprocessor system comprising:

a plurality of modules (Fig. 1, elements 2-5) including a microprocessor (Fig. 1, element 2; Fig. 2, element 12) and at least one storage module (Figs. 1 and 2, element 3) for storing code and data for the microprocessor, at least one of the modules (Figs. 1 and 2, element 3, memory 7) storing a serial number of the at least one module in a non-exchangeable manner (Specification, p. 4, l. 15-26);

an arrangement for storing a code number (Figs. 1 and 2, element 3, memory 6), the code number being obtained from the serial number by using an encryption method (p. 2, l. 9-

12), and for storing information required to calculate the serial number from the code number (p. 5, l. 5-9),

wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information (p. 5, l. 5-9), to compare the calculated serial number to the stored serial number (p. 5, l. 10-12), and to execute or not execute at least part of the code as a function of a result of the comparison (p. 5, l. 12-16).

With respect to independent claim 10, the present invention provides a method for detecting an exchange of a module, identified by a serial number, in a microprocessor system, the method comprising:

storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number (p. 2, l. 9-15);

reading the code number and calculating an unencrypted serial number from the code number with the aid of the information (p. 5, l. 5-9);

comparing the decrypted serial number thus obtained with the serial number of the module (p. 5, l. 10-12); and

detecting an exchange of the module if the serial number of the module does not match the decrypted serial number (p. 5, l. 10-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejections are presented for review on appeal in this case:

(A) Whether pending claims 1, 9, 10 and 17 under 35 U.S.C. § 102(b) are anticipated by U.S. Patent No. 5,771,287 ("Gilley").

(B) Whether pending claims 2-8, 11-16, 18 and 19 are rendered unpatentable under 35 U.S.C. § 103(a) over Gilley in view of U.S. Patent No. 6,026,293 ("Osborn").

VII. ARGUMENTS

A. Rejection of Claims 1, 9, 10 and 17 under 35 U.S.C. § 102(b)

Claims 1, 9, 10 and 17 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,771,287 ("Gilley"). Applicants respectfully submit that the rejection should be withdrawn for at least the following reasons.

To anticipate a claim under § 102(b), a single prior art reference must identically disclose each and every claim element. See Lindeman Machinenfabrik v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984). If any claimed element is absent from a prior art reference, it cannot anticipate the claim. See Rowe v. Dror, 112 F.3d 473, 478 (Fed. Cir. 1997). Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claim invention, arranged exactly as in the claim. Lindeman, 703 F.2d 1458 (Emphasis added). Additionally, not only must each of the claim limitations be identically disclosed, an anticipatory reference must also enable a person having ordinary skill in the art to practice the claimed invention, namely the inventions of the rejected claims, as discussed above. See Akzo, N.V. v. U.S.I.T.C., 1 U.S.P.Q.2d 1241, 1245 (Fed. Cir. 1986).

Independent claim 1 recites, in relevant parts, "a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing **a serial number of the at least one module** in a non-exchangeable manner; an arrangement for storing a code number, **the code number being obtained from the serial number by using an encryption method**, and for storing information required to calculate the serial number from the code number, wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison." Claim 10 recites substantially similar method features as the above-recited features of claim 1.

In support of the rejection, the Examiner contends in the Advisory Action of March 19, 2008, that "Gilley et al. in fact discloses that the microprocessor is adapted to **calculate a serial number** (a present authentication code) (column 6, lines 18-22) **from the code number** (secret key) on the basis of the information (column 6, lines 18-22)." However, to the extent the Examiner is attempting to address the claimed limitation of "**the code number being obtained from the serial number by using an encryption method**," the Examiner's contention is clearly the exact opposite of the claimed limitation, i.e., the Examiner explicitly

states that the serial number (PAC) is obtained **from** the code number (SK), and this is exactly what is stated in the section cited by the Examiner: "The term 'present authentication code' (or 'PAC') refers to a value which is calculated by using the SK [secret key] of the scrambler and the present OMC found in the EEPROM." (Col. 6, l. 18-20).

Applicants note that the above-recited assertion made by the Examiner in the Advisory Action is similar to the assertions made in the Final Office Action of November 7, 2007, i.e., the Examiner contended in the Final Office Action: a) the "authentication code" in Gilley is equivalent to the "serial number" recited in claim 1; and b) in support of the assertion that Gilley teaches the claimed feature of "the **code number** being obtained **from the serial number by using an encryption method**," the Examiner cited col. 5, l. 65 - col. 7, l. 1 of Gilley as disclosing a "secured encryption algorithm is used with the operation mode code and the secret key to **create** the authentication code."

For at least the foregoing reasons, it is absolutely clear that Gilley does not disclose or suggest the "**code number being obtained from the serial number by an encryption method**"; instead, Gilley discloses the exact opposite, i.e., **the serial number (authentication code)** is obtained **from the secret key**.

To the extent the Examiner may be simply ignoring the claimed limitation of the "**code number being obtained from the serial number by an encryption method**" as being an error and/or contradictory to the additional claimed limitation of "storing information required to calculate the serial number from the code number, wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information," Applicants note that the above-recited limitations are two separate and distinct features which are not contradictory.

For at least the foregoing reasons, claims 1 and 10, as well as their dependent claims 9 and 17, are patentable over Gilley. Reversal of the anticipation rejection is respectfully requested.

B. Rejection of Claims 2-8, 11-16, 18 and 19 under 35 U.S.C. § 103(a)

Claims 2-8, 11-16, 18 and 19 were rejected under 35 U.S.C. § 103(a) as obvious over Gilley in view of U.S. Patent No. 6,026,293 ("Osborn"). Applicants respectfully submit that the rejection should be withdrawn, for at least the following reasons.

In order for a claim to be rejected for obviousness under 35 U.S.C. § 103(a), the prior art must teach or suggest each element of the claim. See Northern Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296 (1990); In re Bond, 910 F.2d 831, 834 (Fed. Cir. 1990). To establish a *prima facie* case of obviousness, the Examiner must show, *inter alia*, that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the references, and that, when so modified or combined, the prior art teaches or suggests all of the claim limitations. M.P.E.P. §2143. In addition, as clearly indicated by the Supreme Court, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the [prior art] elements" in the manner claimed. See KSR Int'l Co. v. Teleflex, Inc., 127 S. Ct. 1727 (2007). To the extent that the Examiner may be relying on the doctrine of inherent disclosure for the obviousness rejection, the Examiner must provide a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics necessarily flow from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; see also Ex parte Levy, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Claims 2-8, 11-16, 18 and 19 depend from claim 1 or claim 10. As noted above, Gilley fails to anticipate parent claims 1 and 10. In addition, Osborn clearly does not overcome the deficiencies of Gilley as applied against claims 1 and 10. Therefore, even if one assumes for the sake of argument that there is some motivation to combine the teachings of Osborn and Gilley (which is not conceded), the combination clearly fails to render dependent claims 2-8, 11-16, 18 and 19 obvious. Reversal of the obviousness rejection is requested.

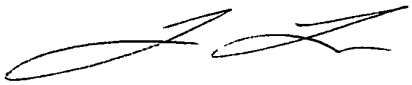
VIII. CONCLUSION

For the foregoing reasons, it is respectfully submitted that the final rejection of claims 1-19 should be reversed.

Claims Appendix, Evidence Appendix and Related Proceedings Appendix sections are found in the attached pages.

Respectfully submitted,

KENYON & KENYON LLP


(R. No. 36,197)

Dated: September 2, 2008

By: SONG LEE for Gerard Messina

Gerard A. Messina
Reg. No. 35,952
One Broadway
New York, New York 10004
(212) 425-7200
CUSTOMER NO. 26646

CLAIMS APPENDIX

The claims involved in this appeal, claims 1-19, in their current form after entry of all amendments presented during the course of prosecution, are set forth below:

1. A microprocessor system comprising:

a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner;

an arrangement for storing a code number, the code number being obtained from the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number,

wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison.

2. The microprocessor system according to claim 1, wherein the encryption method is asymmetrical, the code number is calculated from the serial number with the aid of a secret key, and the information includes a public key as well as a program code for calculating the serial number from the code number.

3. The microprocessor system according to claim 2, wherein one of the at least one module identified by the serial number is a storage module.

4. The microprocessor system according to claim 3, wherein the code number is stored in a same storage module as the serial number.

5. The microprocessor system according to claim 3, wherein the storage module is an electrically rewritable, non-volatile memory, and the code to be executed if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module.

6. The microprocessor system according to claim 1, wherein one of the at least one module identified by the serial number is the microprocessor.

7. The microprocessor system according to claim 1, wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number.

8. The microprocessor system according to claim 7, wherein the different storage module is connected to the microprocessor in a non-separable manner.

9. The microprocessor system according to claim 1, wherein at least two of the modules are each identified by a serial number and the code number is obtained by joint encryption of the serial numbers.

10. A method for detecting an exchange of a module, identified by a serial number, in a microprocessor system, the method comprising:

storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number;

reading the code number and calculating an unencrypted serial number from the code number with the aid of the information;

comparing the decrypted serial number thus obtained with the serial number of the module; and

detecting an exchange of the module if the serial number of the module does not match the decrypted serial number.

11. The method according to claim 10, wherein an asymmetric encryption method is used and a public key of the encryption method is included in the information required to calculate the serial number from the code number.

12. The method according to claim 10, wherein the module is a storage module of the microprocessor system.

13. The method according to claim 12, wherein the code number is stored in the same storage module as the serial number.

14. The method according to claim 12, further comprising deleting a content of the storage module if an exchange of the module has been detected.

15. The method according to claim 10, wherein the module includes a microprocessor of the microprocessor system.

16. The method according to claim 10, wherein at least the information required for calculating the serial number is stored in a different storage module than the code number.

17. The method according to claim 10, wherein the method is used for a plurality of modules of the microprocessor system and the code number is obtained by a joint encryption of serial numbers of the plurality of modules.

18. The method according to claim 10, wherein steps of the method are executed upon each start-up of the microprocessor system.

19. The method according to claim 10, wherein steps of the method are periodically executed during operation of the microprocessor system.

EVIDENCE APPENDIX

In the present application, there has been no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132, or other evidence entered by the Examiner and relied upon by Appellants in the present appeal.